Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 53 (2013) 463 – 471

Procedia Engineering

www.elsevier.com/locate/procedia

Malaysian Technical Universities Conference on Engineering & Technology 2012, MUCET 2012
Part 3 - Civil and Chemical Engineering [553-560]

Secured and Robust Information Hiding Scheme

N.H.Abdul-mahdi[a,]*,A.Yahya[a], R.B.Ahmad[a] and O.M.Al-Qershi[b]

[a] *University Malaysia Perlis (UniMAP)*
School of Communication and Computer Engineering

[b] *School of Electrical & Electronic Engineering*
University of Science Malaysia (USM)

Abstract

The sensitivity of the digital work made it susceptible to many accidental dangers. Accordingly, it has become necessary for the secret data to be protected, identified and extracted. As a result, many researchers have exerted much of their time and efforts in an attempt to find suitable ways for data hiding. As a case in point is the development of steganography, a technique used for hiding the important information imperceptibly. As far as the present work is concerned, the researcher adopts the steganography system for the purpose of embedding secret data within the frequency domain. Such a step can be done by modifying the DCT coefficients in a content-based manner, so that the embedding map will be able to easily identify the embedding blocks; a matter which in turn helps recover the data hidden in the frequency domain. The arrived at results reflected the manageability of the system to fight against AWGN and JPEG compression attacks and a high quality stego-images. However, being only part of an image is used for the purpose of hiding data has limited the capacity of the system in this regards.

Selection and peer-review under responsibility of the Research Management & Innovation Centre, Universiti Malaysia Perlis

1. Introduction

In this modern era, computers and the internet are major communication media that bring the different parts of the world into one global virtual world. As a result, people can easily exchange information and distance is no longer a barrier to communication. However, the safety and security of long-distance communication remains an issue. This is particularly important in the case of confidential data. The need to solve this problem has led to the development of steganography schemes. Steganography is a powerful security tool that provides a high level of security; particularly when it is combined with cryptography [1].Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the presence of the message itself from an observer. Steganography does not replace cryptography; it rather enhances the security using its obscurity features.

Steganography is the art and science of concealing information in an appropriate multimedia carrier, like, image, audio and video files. It comes under the supposition that if the feature is visible, the point of attack is evident. Therefore, the goal here is always to hide the very existence of the embedded data [2].

Steganography has many useful applications, e.g.in the copyright control of materials, enhancing robustness of image search engines and in smart IDs (identity cards) where individuals' details are embedded in their photographs. Steganography can be characterized by three factors: undetect ability (imperceptibility), robustness, and hiding capacity

* Corresponding author. *E-mail address:*

Selection and peer-review under responsibility of the Research Management & Innovation Centre, Universiti Malaysia Perlis
doi:10.1016/j.proeng.2013.02.060

[2].It is not possible to maximize robustness, imperceptibility, and capacity simultaneously. Therefore, an acceptable balance of these items must be met by the application. When Steganography is used as a method for hiding communication, imperceptibility becomes the most important requirement while robustness and possibly capacity can be sacrificed [4].A number of ways exist to hide information in digital images. Some of the common approaches include: Least significant bit insertion (LSB), Masking and filtering, and Algorithms and transformations. Each of these techniques can be applied, with varying degrees of success, to different image files [5].For instance, LSB manipulation is a quick and easy way for hiding information; however, is vulnerable to small changes resulting from either the process of image processing or from the lossy compression. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than being a mere hidden message in the "noise" level. Consequently, masking techniques are more robust than LSB insertion with respect to compression, cropping, and to some image processing. Hence, they are more suitable for use in digital watermarking [6].

Other more robust methods of hiding information in images include applications that involve a manipulation in the mathematical functions and image transformations. The widely used transformational functions include Discrete Cosine Transformation (DCT), Discreet Fourier Transform (DFT), and Discreet Wavelet Transformation (DWT) [7-12]. The basic approach to hiding information with DCT, DFT or DWT involves transforming the cover image, tweaking the coefficients, and then inverting the transformation. If the choice of coefficients is good and the size of the changes manageable, then the result will be very close to the original [7].

Recently, Mali et al. proposed a robust DCT-based steganographic scheme via using a powerful coding framework that allows the dynamic choice of hiding locations and the embedding of low and medium DCT coefficients [13]. The robustness of this scheme not only comes from exploiting low and medium DCT coefficients, but also comes mainly from the redundancy.The payload bits are repeated (n) times in order to add robustness to the system. However, the scheme has a sever drawback that results in a loss of information. In this paper, Mali et al.'s scheme and its drawbacks will be first presented. Then, a proper modification is proposed to overcome the adopted scheme drawbacks and make it more applicable via using the embedding map.

2. Related Work

DCT has been used widely for steganography and watermarking purposes. DCT-based methods hide data bits in significant areas of the cover-image; a technique that makes them more robust to attacks. Generally, DCT is applied to image blocks of 8×8 pixels, and selected coefficients are used to hide data bits. The coefficients are modified differently in order to reflect an embedding of "0" or "1".

Mali et al. [13] presented a robust and secured method for embedding a high volume of text information in digital cover-images without leaving perceptual distortion. It has been found that this method is robust against intentional or unintentional attacks. As cases in point are the following: image compression, tampering, resizing, filtering and Additive White Gaussian Noise (AWGN). Figure 1 shows the steganographic data hiding system proposed by Mali et al. Mali et al.'s scheme consists of two main stages: processing the data to be embedded and embedding the data. In the first stage, the pure payload bits undergo three processes:

1- Encryption: in order to secure the data;
2- redundancy addition: to reduce the bit error rate (BER); and
3- Interleaving: to ensure that the redundant bits are spread all over the image.

The details about these steps will not be gone through. In this stage, both redundancy and interleaving are responsible for the recovery of the robust data at the receiver end. However, the overall robustness depends also on the embedding procedures. For this reason, the embedding procedures and their drawbacks are discussed in the following section.

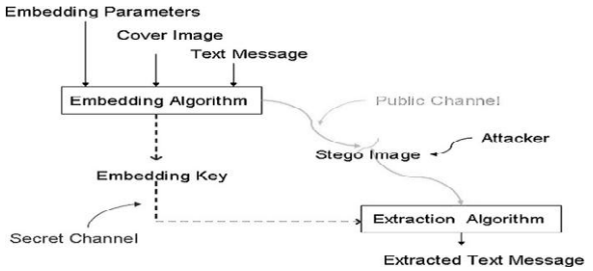

Fig.1. General steganographic system proposed by Mali et al. [13]

2.1. Mali et al. 's Data Hiding Scheme

The inputs to the embedding system are Cover-image file (*C*), the processed text (*FBS*), Energy Threshold Factor ($\hat{w}$), and JPEG quality factor (QF).The embedding phase can be summarized in the following section. The reader can refer to the original paper for additional details.

Step 1:	Divide the image into 8×8 non-overlapping blocks so thatDCT is appliedto each block a_{ij} to getC_{ij} as: $$C_{ij} = DCT(a_{ij}) \quad (1)$$ Where $i, j = \{0, 1, 2, \dots\dots, 7\}$
Step 2:	Calculate the Energy of each block as: $$E = \sum_{i=1}^{7}\sum_{j=1}^{7} \|C_{ij}\|^2 \; \forall i, j = \{0, 1, 2, \dots\dots\dots, \quad 7\}, (i, j) \neq 0 \quad (2)$$
Step 3:	Calculate the Mean Value of Energy (MVE) of the image using the equation: $$MVE = \frac{1}{B}\sum_{1}^{B} E_b \quad (3)$$ where$B$= Total number of blocks and b= block number.
Step 4:	Identify the Valid Blocks VBs,which satisfy the Energy Threshold Criteria$\geq E_T$, where $E_T = \hat{w} \times MVE$.
Step 5:	The coefficients of all *VBs* are quantized by dividing them according to their respective elements of quantization matrix as, $$\hat{C_{ij}} = \frac{C_{ij}}{M_{ij}^{QF}} \forall i, j = \{0, 1, \dots\dots, 7\} \quad (4)$$ where, $\hat{C_{ij}}$ is the quantized coefficient matrix, M_{ij}^{QF} is the $ijth$ element of the quantization matrix for a given value of *QF*.
Step 6:	Identify the Valid DCT Coefficients (*VC*s), which satisfy the non-zero criteria ($C_{ij} \neq 0$)and which fall into the lower and middle frequency band.
Step 7:	The coefficients of all *VC*s are scanned in a zigzag fashion to get one dimensional vector C_k. The process of embedding data will then be done via changing the quantized non-zero DCT coefficients, where the odd value for '*bit* = 0' or the even value for '*bit* = 1'. The coefficients with the hidden bits d_k are given by, $$\hat{d_k} = \begin{cases} Odd\hat{C_k}, if bit = 0 \\ Even\hat{C_k}, if bit = 1 \end{cases} \quad (5)$$
Step 8:	The hidden coefficients $\hat{d_k}$ are reversely scanned to form an 8 × 8 matrix. It will then be multiplied by the JPEGQuantization matrix to obtain unquantified coefficientsC_{ij}.
Step 9:	Apply inverse DCTto each block, and reconstruct the image as Stego-image.

From the steps above, it is obvious that the extraction phase depends on identifying the blocks that have been used for the correct embedding. Misidentifying those blocks will cause losing a portion of the embedded data or extracting the rubbish. During the extracting phase, the blocks that have been used for embedding data should be identified. Such a process is achieved by following two steps:

First: The energy of the block should be $\geq E_T$ (step 4).

Second: The lower and middle DCT Coefficients of the block should satisfy the non-zero criteria (step 6). If the algorithm fails at identifying the blocks in any of the steps, the embedded data is extracted incorrectly.

In the current study, Mali et al.'s algorithmhas been implemented, and simulated using different images and randomly generated secret data. The results showed that the algorithm may misidentify the blocks in some cases. For example, in one of the experiments on the standard image 'Lena', it has been noticed that the embedding process changed the MVE and$E$ values as illustrated in Fig. 2. As a result, the embedded block failed to be identified during the extraction phase because$E$was less than E_T. In another situation, reconstructing the stego-image involved a rounding operation to get the integer pixel values. The rounding operation might turn some of non-zero coefficients to zero coefficients or vice versa. This also led to misidentify the blocks, which carry the data. Table I illustrates the number of misidentified blocks after applying the Mali et al.'s algorithm on image 'Lena' using different quality factor values (QF) and different energy threshold values ($w^{\wedge}$). Such a problem may affect the integrity of the embedded data; especially, when one cannot identify which blocks have been misidentified. In order to solve the problem of blocks misidentification, an embedding map (location map) is proposed in this regard. The concept of the embedding map has been used in many data hiding techniques to identify correctly the location of the blocks or regions where data has been embedded. That is to say, not the whole image has been used for embedding [14-15]. In the following section, Mali et al.'s algorithm is modified by incorporating an embedding map.

71	70	83	85	79	80	58	83
66	61	75	73	70	77	70	92
73	68	72	69	73	81	85	103
81	66	76	65	76	94	97	111
85	65	89	84	84	104	109	116
83	65	86	92	96	119	125	127
86	66	97	109	105	126	140	134
100	82	111	119	112	135	148	135

(a) MVE= 565,670 and E = 568,185, $w^{\wedge} = 1 \rightarrow E > E_T$

71	68	75	85	75	75	67	81
71	67	75	80	73	74	77	88
77	78	75	79	81	80	90	100
78	74	75	69	82	92	100	112
80	75	85	81	88	99	109	121
80	81	84	88	100	112	122	133
77	81	95	105	113	121	135	141
81	91	105	114	122	131	143	144

(b) MVE = 566,780 and E = 560,244

$w^{\wedge} = 1 \rightarrow E < E_T$

Fig. 2. Example of undetected block because E <MVE: (a) the original block, (b) after embedding.

3. The proposed Data Hiding Scheme

The proposed algorithm is based mainly on Mali et al.'s algorithm. In order to overcome the problem of blocks misidentification, an embedding map technique is introduced to assure extracting the embedded data correctly. Exploiting an embedding map implies generating a binary map of a size equal to the number of blocks in the image. If the image size is $\boldsymbol{m} \times \boldsymbol{n}$,then, the embedding map size is $\frac{\boldsymbol{m}}{\boldsymbol{8}} \times \frac{\boldsymbol{n}}{\boldsymbol{8}}$, where the block size is $\boldsymbol{8} \times \boldsymbol{8}$ pixles. Each block in the image is represented by a bit in the embedding map, and if the bit is '1', this means that the corresponding block is used for embedding data and vice versa. The embedding map will be concealed in specific regions of the image while the data is concealed in different regions. The regions, i.e. the blocks, in which the data is hidden are determined according to Mali et al.'s method. The embedding map can be embedded in some predefined regions selected by the user. However, this option may affect the security of the data because the same regions are used every time. So, it is preferable to adopt a more secure way to hide the embedding map, as described in the next section.

3.1.Hiding the Embedding Map

The embedding map is necessary to initiate the extracting phase. This means that the embedding map must be concealed in the image in such a secure and robust way. To achieve these requirements, two powerful techniques are used. The first technique is used to guarantee the security of the embedding map. This step is done by selecting the regions to be embedded in such a dynamic way, depending on the key-points of the image. For this purpose, Speed-Up Robust Features (SURF) is used. The SURF is used to extract the distinctive local features in the image and to produce the key-point descriptors that present those features. Those feature vectors/descriptors are invariant to rotation, translation, and scaling; they are further partially invariant to illumination changes and are robust to local geometric distortion [16]. Each feature vector has some information that describes its corresponding key-point. The important part of the information for the algorithm is the coordinates of the center of the key-point and its scale. Twelve non-overlapped key-points with the highest scales are selected and used for hiding the embedding map. These key-points are the most robust features in the image and can be detected even when the stego-image undergoes different types of operations, such as JPEG compression and Gaussian noise. For the second requirement, the robustness, a DWT-based embedding technique is adopted in which the data is embedded in a content-based manner. For more details on using SURF and the content-based embedding, the reader can refer to [17,18].

3.2. Secret Data Embedding Phase

With the introduced embedding map, the proposed algorithm can be describedthrough the following steps:

- The SUR is applied to the image, and 12 key-points with highest scales are identified. Each key-point defines a square region of the size 32×32 pixels, which has the same center coordinates. The 12 square regions are used for hiding the embedding map.
- Divide the image into 8×8 non-overlapping blocks so that DCT is appliedto each block a_{ij} to get C_{ij}, as in Equation (1). Notice that the blocks that intersect with the 12 square regions and obtained in Step 1 are discarded as those regions are used for hiding the map not for the data.
- Scan the blocks and find the blocks that can be used for embedding (according to Mali et al.'s algorithm), as described in section 2.1.
- Build an embedding map to indicate the blocks in which the data bits will be embedded.
- The secret data is embedded in the blocks defined in Step 3 by modifying the DCT coefficients according to Mali et al.'s algorithm.
- The embedding map is embedded in the 12 square regions defined in Step 1 by modifying the DWT coefficients (in a content base manner), as described in section 3.1. Adding the redundancy bits and interleaving techniques are then used to prepare both data and the embedding map to be hidden.

4. Experimental Studies

To assess the performance of the proposed algorithm, experiments have been done on three standard grayscale images; 'Lena', 'Boat', 'and 'Gold hill', with the size $\mathbf{512 \times 512}$. In order to evaluate the reliability of the proposed algorithm compared to Mali et al.'s algorithm, different attacks of different levels were applied on the stego-image. The attacks involved are JPEG compression and Gaussian Additive noise (AWGN). A comparison between the proposed algorithm and Mali et al.'s algorithm in terms of reliability (number of missed blocks) is presented in Tables II and III.

It is worth mentioning that the number of missed blocks can be calculated by subtracting the number of the detected blocks in the receiving end from the blocks that have been used for secret data embedding (the actual embedding blocks). Accordingly, when the number of the detected blocks is less than the actual number of the embedding blocks, the result will be a positive number. On the other flip, due to the applied attacks to the stego-image, erroneous blocks may be detected. As a result, the number of the detected blocks may be more than the actual number of embedding blocks. This is the reason behind having numbers with negative values about the misidentified blocks, as shown in Tables II and III.

On the other hand, the visual quality of the obtained stego- image with the proposed algorithm is compared to that with Mali et al.'s one. For more illustration about this comparison, consider Table IV. The visual quality is measured by the Peak Signal to Noise Ratio (PSNR), as given in (6)

$$PSNR(I, I_S) = 10\, log_{10} \frac{{MAX_I}^2}{\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I(i,j)-I_{S(i,j)}\right\|^2} \tag{6}$$

Where $I$is the original image; I_S is the stego-image; MAX_I is the maximum possible pixel value of the image I. The obtained results show that the proposed algorithm has a better visual quality .For the purpose of evaluation, another comparison is accomplished in terms of the hiding capacity. The capacity is measured by examining the number of payload bits that can be embedded in the image and retrieved successfully. The obtained results are shown in Table V.

5. Discussion and Conclusions

In this paper, an interesting algorithm proposed by Mali et al. is reviewed. Their algorithm shows adequate levels of robustness due to combining DCT and adding redundancy bits. However, some of the blocks that carry data might be misidentified during the extraction process. The present paper aims at enhancing the reliability of the original algorithm by overcoming the problem of the misidentified blocks. To do so, an embedding map has been adopted to indicate the location of the blocks, which have been used for embedding. This means that some regions of the image will be exploited for hiding data while some others will be used for hiding the embedding map. The blocks in which the data is concealed are determined according to Mali et al.'s algorithm. The regions in which the embedding map is concealed are determined in such a dynamic way to increase the security of the algorithm. This goal has been achieved via using the SURF technique, which is used to find the robust key-points of the image, no doubt that each image has different key-points. The embedding map is embedded in those regions using a DWT-based method.

Obviously, the experimental results in Tables II and III show that the proposed algorithm can overcome the problem of blocks misidentification even when the stego-image undergoes JPEG compression or Gaussian noise. The high reliability of the algorithm in identifying the blocks comes from the ability of SURF to detect the key-points even after applying the attacks. Besides, the DWT-based embedding technique plays an important role in keeping the embedding map intact. However, strong attacks, such Gaussian noise may cause the blocks to be slightly misidentified, as it is the case in the image of 'Boat' in Table IV.

In comparison to Mali et al.'s algorithm, the proposed algorithm shows a better visual quality in terms of PSNR, as shown in Table 4. Such a process can be achieved for the images used for testing and with all energy threshold values used($\hat{w}$). However, Table Vindicates that the hiding capacity of the proposed scheme is rather lower than what achieved by Mali et al.'s algorithm. The reason behind the reduction in the capacity is due to exploiting some regions of the image for hiding the embedding map.

So far, the robustness of the algorithm in terms of Bit Error Rate (BER) has not been tackled. This is because the same embedding technique used in Mali et al.'s algorithm for hiding the data has been used in the present study. This means that both algorithms have the same level of robustness. Moreover, at the present study further aims at enhancing the reliability of Mali et al.'s algorithm. Increasing the robustness is out of the scope of this paper.

The experimental results show the ability of the new algorithm to overcome the problem of losing data even with JPEG compression or Gaussian noise. However, exploiting the embedding map reduces the available hiding capacity. To increase

the available hiding capacity, more embedding techniques with high hiding capacity should be considered to hide the embedding map. This will permit more data (message) to be embedded in the image and retrieved effectively. Moreover, more possible attacks are to be investigated.

Table 1. Misidentifiedblocksafterapplyingmali'salgorithm On Image 'Lena'

		Number of misidentified blocks			Percentage of misidentified blocks		
		QF= 50%	QF= 75%	QF = 100%	QF = 50%	QF = 75%	QF = 100%
$w^{\wedge}$	0.5	35	27	51	%1.17	%0.90	%1.71
	0.6	30	28	47	%1.11	%1.03	%1.73
	0.7	35	27	39	%1.39	%1.07	%1.55
	0.8	21	23	44	%0.90	%0.98	%1.88
	0.9	42	14	39	%2.00	%0.67	%1.85
	1	18	21	40	%0.98	%1.15	%2.19

Table 2.
A Comparison Between The Proposed Algorithm And Mali's Algorithm In Terms Of Reliability With (Qf = 75% &$W^{\wedge}$ = 0.5)

	Number of misidentified blocks					
	The proposed algorithm			Mali's Algorithm		
	Lena	Boat	Gold hill	Lena	Boat	Gold hill
No attack	0	0	0	27	15	17
JPEG 100%	0	0	0	-14	-9	-5
JPEG 80%	0	0	0	316	249	228
Gaussian Noise 45dB	0	0	0	-26	-12	-5
Gaussian Noise 35dB	0	0	0	-32	-12	2

Table 3.
A Comparison Between The Proposed Algorithm And Mali's Algorithm In Terms Of Reliability With (Qf = 75% &$W^{\wedge}$ = 0.8)

	Number of misidentified blocks					
	The proposed algorithm			Mali's Algorithm		
	Lena	Boat	Gold hill	Lena	Boat	Gold hill
No attack	0	0	0	23	14	32
JPEG 100%	0	0	0	-12	-3	6
JPEG 80%	0	0	0	250	247	175
Gaussian Noise 45dB	0	0	0	-31	-12	10
Gaussian Noise 35dB	0	16	0	-28	-20	2

Table 4.
A Comparison Between The Proposed Algorithmand Mali's Algorithmin Termsof Psnr

		PSNR values (dB) at QF = 75%					
		The proposed algorithm			Mali's Algorithm		
		Lena	Boat	Gold hill	Lena	Boat	Gold hill
$\hat{w}$	0.5	37.28	34.10	36.42	33.19	32.66	33.36
	0.6	37.62	34.24	36.98	33.56	32.78	33.82
	0.7	38.33	34.67	37.61	33.91	32.94	34.28
	0.8	38.37	35.10	38.51	34.22	33.18	34.89
	0.9	38.79	35.74	39.18	34.69	33.53	35.58
	1	39.74	36.76	39.53	35.31	34.16	36.57

Table 5.
A Comparison Between The Proposed Algorithmand Mali's Algorithmin Terms Of Hiding Capacity

		Hiding Capacity (bits)					
		The proposed algorithm			Mali's Algorithm		
		Lena	Boat	Gold hill	Lena	Boat	Gold hill
$\hat{w}$	0.5	25,536	46,144	30,016	83,664	93,996	80,304
	0.6	22,400	44,352	25,536	75,936	91,196	72,072
	0.7	19,264	38,976	21,056	70,476	87,892	64,344
	0.8	18,816	33,152	16,128	65,688	83,272	56,196
	0.9	15,680	25,088	12,096	58,884	76,580	47,796
	1	11,648	16,128	10,752	51,212	66,724	38,444

References

[1] S.A. Halim and Sani M.F.A.Sani,"Embedding using spread spectrum image steganography with GF (2^m)".In Proc. IMT-GT-ICMSA 2010; 659-666.

[2] A. Cheddad, "Steganoflage: A new image steganography algorithm". Ph.D. Thesis, University of Ulster, 2009.

[3] A. Cheddad, J. Condell, K. Curran, and P.M. Kevitt," Digital image steganography: Survey and analysis of current methods". *Signal Processing,* vol. 90, pp. 727–752, 2010.

[4] B. Li, J. He, J. Huang, and Y. Shi Qing,"A Survey on image steganography and steganalysis".*Journal of Information Hiding and Multimedia Signal Processing,*vol. 2, pp. 123-138, 2011.

[5] N.F. Johnson and S. Jajodia,"Exploring steganography: seeing the unseen". *IEEE Computer Journal,* vol. 31, pp. 26-34, 1998.

[6] K. Curran and K. Baily,"An evaluation of image based steganography methods". *Multimedia Tools and Applications Journal,* vol. 30, pp. 55-88, 2006.

[7] A. Naga, S.D. Biswas, D. Sarkar, and P.P. Sarkar. "A novel technique for image steganography based on Block-DCT and Huffman Encoding". *International Journal of Computer Science and Information Technology,* vol. 2,pp.103-112, 2010.

[8] C.C. Chang, T.S. Chen, and L.Z. Chung , " A steganographic method based upon JPEG and quantization table modification".*Information Sciences,* vol.141, pp. 123-138, 2002.

[9] M. Ashourian, R.C. Jain and Y-H. Ho,"Dithered quantization for image data hiding in the DCT domain". *In proceeding of IST2003*; 171-175.

[10] M. Iwata, K Miyake, and A. Shiozaki, Digital Steganography Utilizing Features of JPEG Images,*IEICE Trans. Fundamentals*, vol. E87-A, pp. 929–936, April 2004.

[11] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressedimages". *Information Sciences*, vol. 177, pp. 2768-2786, July 2007.

[12] C-C Lin and P-FShiu,"High capacity data hiding scheme for DCT-based images". *Journal of Information Hiding and Multimedia Signal Processing,* vol.1, pp. 123-138, 2010.

[13]**S.N.** Mali,P.M. Patil, and R.M. Jalnekar,"Robust and secured image-adaptive data hiding".*Digital Signal Processing,* vol. 22,pp. 314–323, 2010.

[14] J. Tian,"Reversible data embedding using a difference expansion". *IEEE Transactions on Circuits and Systems for Video Technology,*vol.13, pp.890-896, 2003.

[15] A.M. Alattar,"Reversible watermark using the difference expansion of a generalized integer transform".*IEEE Transactions on Image Processing,*vol.

13,pp.1147 – 1156, 2004.
[16] H. Bay, “From wide-baseline point and line correspondences to 3D”. *Ph.D. Thesis* 2006; Swiss Federal Institute of Technology, Switzerland.
[17] N. Hamid., A. Yahya, R.B. Ahmad, and O.M. Al-Qershi O. “Characteristic region based image steganography using Speeded-Up Robust Features technique”.*IEEInternational Conference on Future Communication Networks, ICFCN* 2012; pp.141-146, 2012.
[18] L. Li, J. Qian, and J-S Pan,“Characteristic region based watermark embedding with RST invariance and high capacity”. *AEU-International Journal of Electronics and Communications,* vol. 65,pp. 435-442, 2011.